# CC and CMMI®

# An Approach to Integrate CC with Development

Wolfgang Peter

TÜV Informationstechnik GmbH

The Trust Provider

- TÜViT -

# Contents

1. Status Quo
2. CMMI® for Development
3. Striking Analogies
4. Combining Standards
5. Conclusion

# What CC does accomplish ...

- assesses and rates security capabilities of IT products
- establishes various levels of confidence in those products
- offers flexibility for new type of products and configurations, and development models
- provides mutual recognition, i.e. dozens of countries and many commercial users buy into working with CC
- ...

# ... but ...

Ø uses a complex and somehow artificial “language” developers are not familiar with

Ø usually starts fairly late in the development process

Ø requires documents “just for CC”

Ø focuses on product features, not on development processes

Ø ...

# Bottom line

Ø CC is normally not integrated with development

Ø CC causes disruption from regular development processes

Ø CC often results in established coexistences of “normal” and “CC development” within organizations

Ø CC is typically not institutionalized within an organization

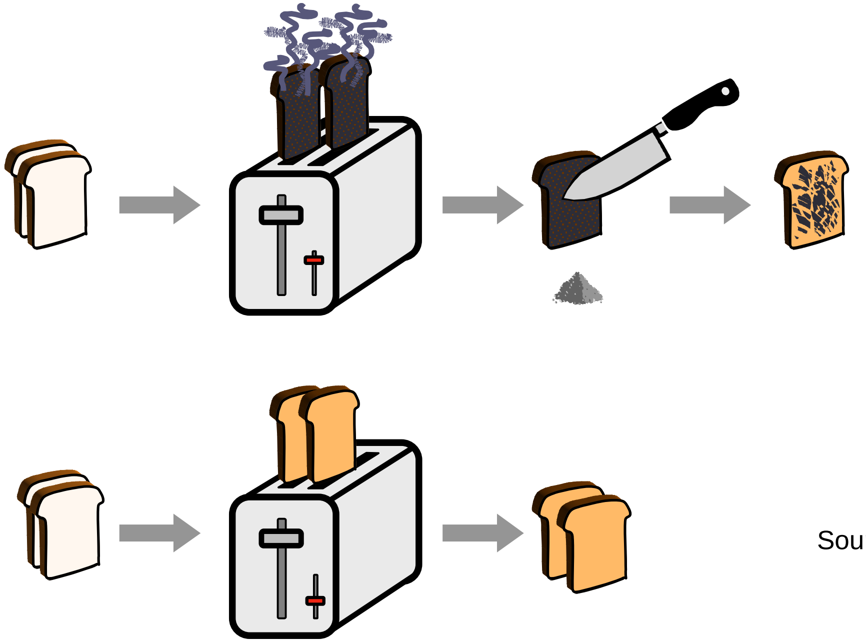
# Associated risks

- CC is normally not integrated with development
- CC causes disruption from regular development processes
- CC often results in established coexistences of "normal" and "CC development" within organizations
- CC is typically not institutionalized within an organization

- Decisions on a case by case basis
- Unnecessary "overhead" Waste of time and money
- No efficient re-usage of development results (specifications, test results, development documents etc.)
- Heavy dependent on individuals No guarantees that historical results can be repeated

# In general ...

- The quality of a product is highly influenced by the quality of the processes used to acquire, develop, and maintain it



Source: SEI, Mastering Process Improvement

- Every organization involved in the development of security products would basically benefit from experiences and best-practices of well-defined and structured engineering standards

# Contents

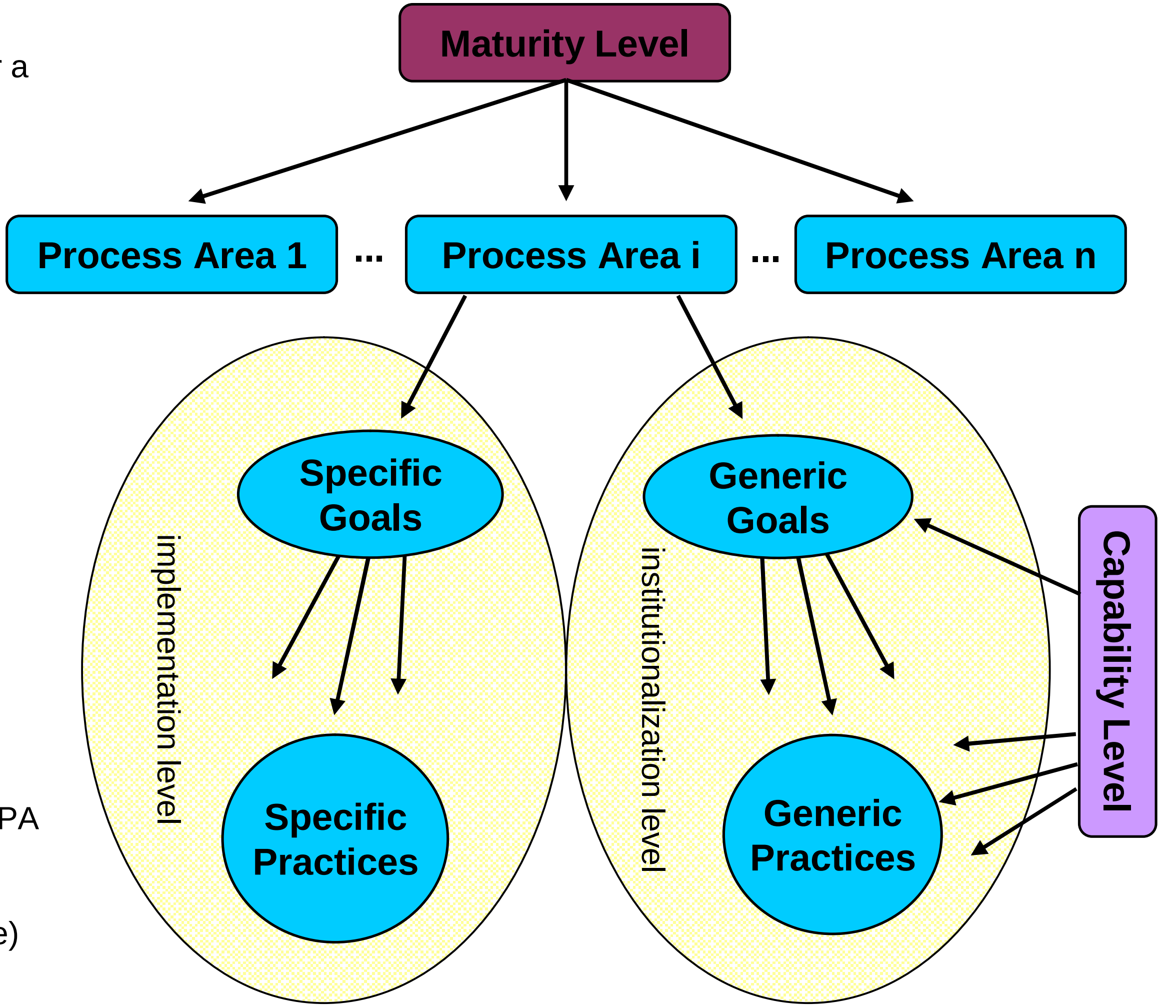
1. Status Quo
2. **CMMI® for Development**
3. Striking Analogies
4. Combining Standards
5. Conclusion

# Background

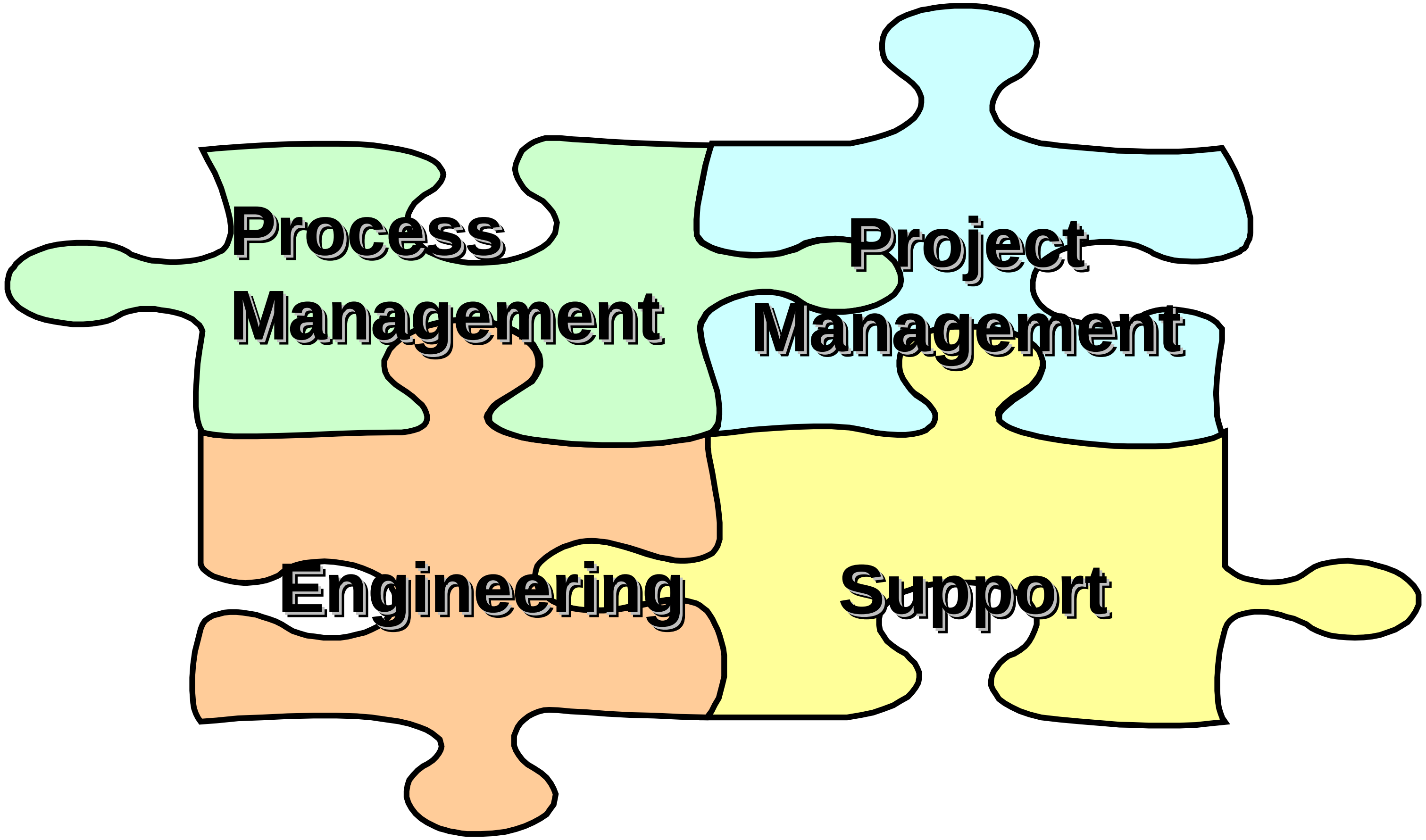
- **CMMI® (Capability Maturity Model® Integration)** is a process improvement approach that provides organizations with the essential elements of effective processes
- Successor of CMM or Software CMM; CMM developed from 1987 through 1997; release of CMMI, V1.1 in 2002
- Created by members of industry, government and the SEI (Software Engineering Institute, Pittsburgh, PA, USA)
- Three models
  - CMMI for Development (CMMI-DEV), Version 1.2 (08/2006)
  - CMMI for Acquisition (CMMI-ACQ), Version 1.2 (11/2007)
  - CMMI for Services (CMMI-SVC), (2009)
- Primary focus: process improvement
  - Organizations cannot be CMMI “certified”, but are appraised and awarded a 1-5 level rating (e.g., using **SCAMPI - Standard CMMI Appraisal Method for Process Improvement)**
- Web Site: http://www.sei.cmu.edu/cmmi/

# Key concept

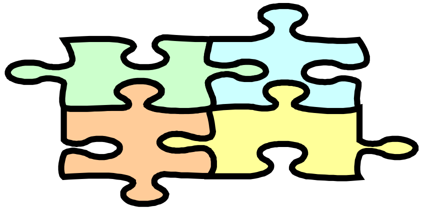
- **Process**
  - sequence of steps performed for a given purpose
- **Process Areas** (PA)
  - characteristics of effective processes
- **Specific/Generic Goals** (SG/GG)
  - requirements
- **Specific/Generic Practices** (SP/GP)
  - expected activities
- 2 types of representations
  - **continuous**
  - **staged**
- **Capability Level** (CL)
  - CL 0, CL 1, ..., CL5 (cumulative)
  - PA specific
  - CL i = achievement of GG i in a PA
- **Maturity Level** (ML)
  - ML 1, ML 2, ..., ML 5 (cumulative)
  - pre-defined set of PAs, each reaching a pre-defined CL



# Continuous representation: Process Areas by categories - 1



# Continuous representation: Process Areas by categories - 2



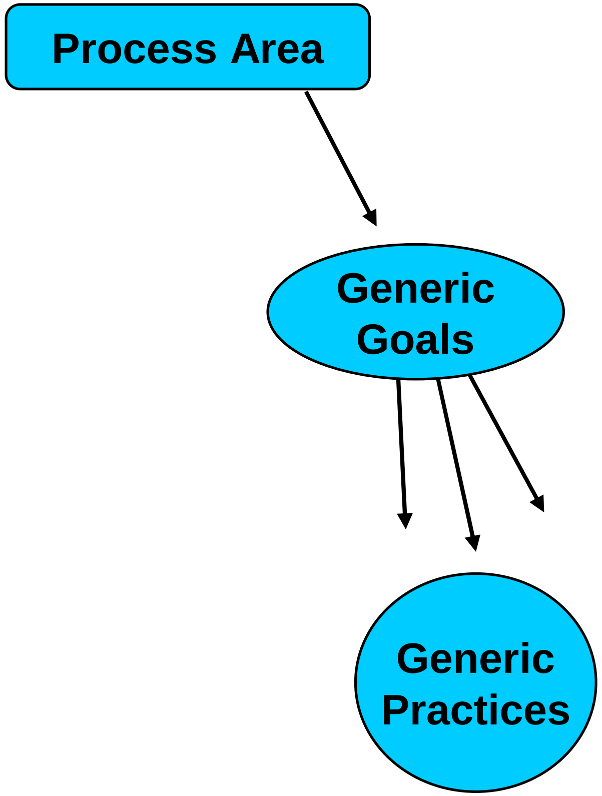
| Project Management | |
|---|---|
| PP | Project Planning |
| PMC | Project Monitoring and Control |
| SAM | Supplier Agreement Management |
| IPM | Integrated Project Management |
| RSKM | Risk Management |
| QPM | Quantitative Project Management |

| Support | |
|---|---|
| CM | Configuration Management |
| PPQA | Process and Product Quality Assurance |
| MA | Measurement and Analysis |
| DAR | Decision Analysis and Resolution |
| CAR | Causal Analysis and Resolution |

| Engineering | |
|---|---|
| REQM | Requirements Management |
| RD | Requirements Development |
| TS | Technical Solution |
| PI | Product Integration |
| VER | Verification |
| VAL | Validation |

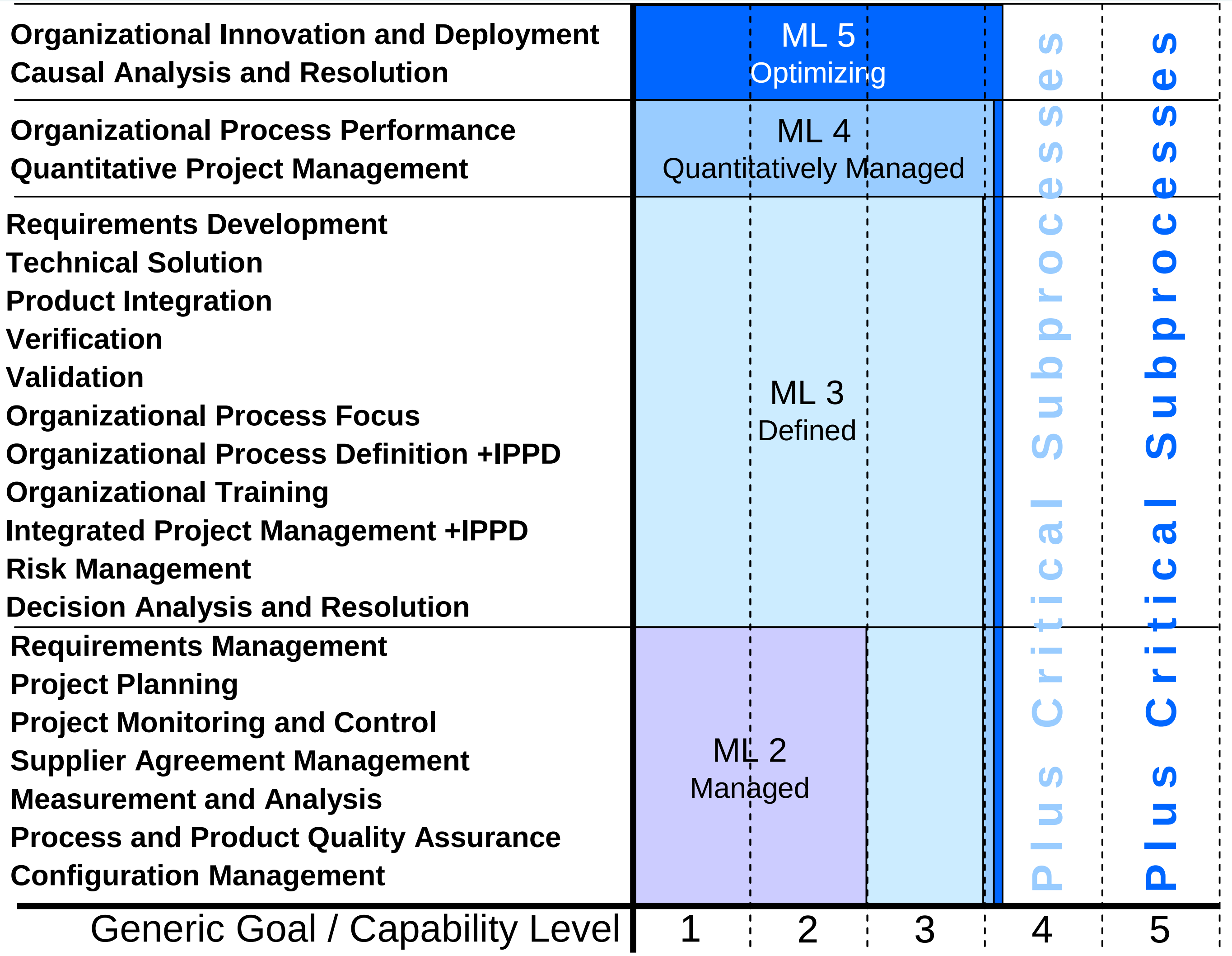
| Process Management | |
|---|---|
| OPF | Organizational Process Focus |
| OPD | Organizational Process Definition |
| OT | Organizational Training |
| OPP | Organizational Process Performance |
| OID | Organizational Innovation and Deployment |

# Generic Goals 1-3



- **GG 1 Achieve Specific Goals**
  - GP 1.1 Perform Specific Practices
- **GG 2 Institutionalize a Managed Process**
  - GP 2.1 Establish an Organizational Policy
  - GP 2.2 Plan the Process
  - GP 2.3 Provide Resources
  - GP 2.4 Assign Responsibility
  - GP 2.5 Train People
  - GP 2.6 Manage Configurations
  - GP 2.7 Identify and Involve Relevant Stakeholders
  - GP 2.8 Monitor and Control the Process
  - GP 2.9 Objectively Evaluate Adherence
  - GP 2.10 Review Status with Higher Level Management
- **GG 3 Institutionalize a Defined Process**
  - GP 3.1 Establish a Defined Process
  - GP 3.2 Collect Improvement Information

# Staged representation: Process Areas by Maturity Level



Organizational Innovation and Deployment
Causal Analysis and Resolution

Organizational Process Performance
Quantitative Project Management

Requirements Development
Technical Solution
Product Integration
Verification
Validation
Organizational Process Focus
Organizational Process Definition +IPPD
Organizational Training
Integrated Project Management +IPPD
Risk Management
Decision Analysis and Resolution

Requirements Management
Project Planning
Project Monitoring and Control
Supplier Agreement Management
Measurement and Analysis
Process and Product Quality Assurance
Configuration Management

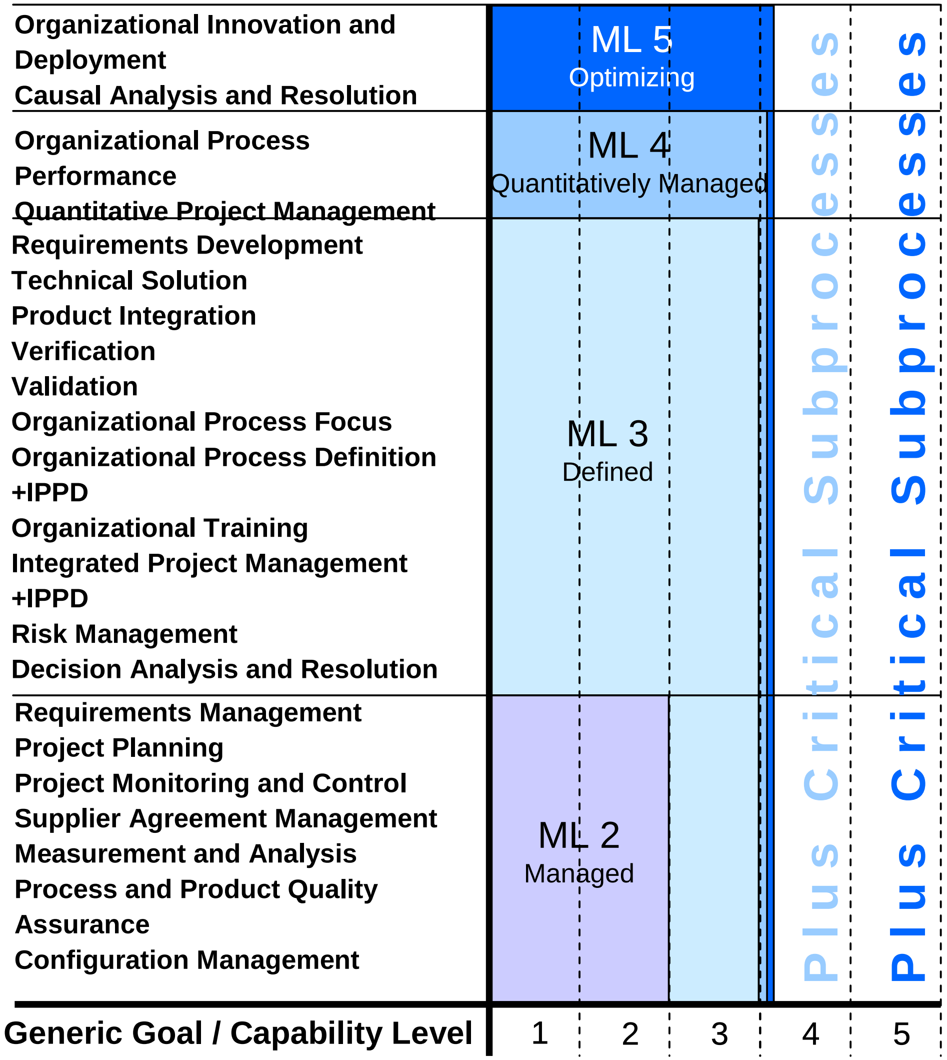
ML 5
Optimizing
ML 4
Quantitatively Managed
ML 3
Defined
ML 2
Managed
Plus Critical Subprocesses
Plus Critical Subprocesses
Generic Goal / Capability Level
1
2
3
4
5

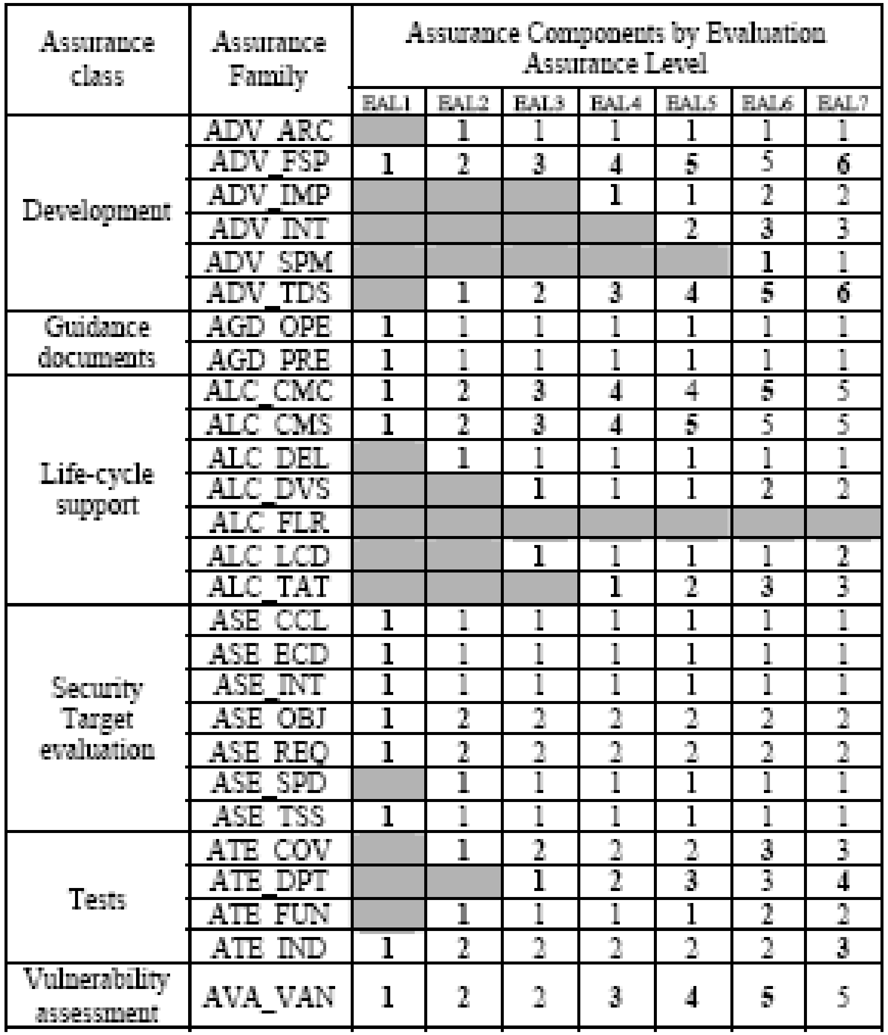
Source: method park, 2008

# Contents

1. Status Quo
2. CMMI® for Development
3. **Striking Analogies**
4. Combining Standards
5. Conclusion

# Look and see!


Organizational Innovation and Deployment
Causal Analysis and Resolution
Organizational Process Performance
Quantitative Project Management
Requirements Development
Technical Solution
Product Integration
Verification
Validation
Organizational Process Focus
Organizational Process Definition +IPPD
Organizational Training
Integrated Project Management +IPPD
Risk Management
Decision Analysis and Resolution
Requirements Management
Project Planning
Project Monitoring and Control
Supplier Agreement Management
Measurement and Analysis
Process and Product Quality Assurance
Configuration Management
ML 5
Optimizing
ML 4
Quantitatively Managed
ML 3
Defined
ML 2
Managed
Plus Critical Subprocesses
Plus Critical Subprocesses
Generic Goal / Capability Level
1
2
3
4
5



| Assurance class | Assurance Family | Assurance Components by Evaluation Assurance Level | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | EAL1 | EAL2 | EAL3 | EAL4 | EAL5 | EAL6 | EAL7 |
| Development | ADV_ARC | | 1 | 1 | 1 | 1 | 1 | 1 |
| | ADV_FSP | 1 | 2 | 3 | 4 | 5 | 5 | 6 |
| | ADV_IMP | | | | 1 | 1 | 2 | 2 |
| | ADV_INT | | | | | 2 | 3 | 3 |
| | ADV_SPM | | | | | | 1 | 1 |
| | ADV_TDS | | 1 | 2 | 3 | 4 | 5 | 6 |
| Guidance documents | AGD_OPE | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | AGD_PRE | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Life-cycle support | ALC_CMC | 1 | 2 | 3 | 4 | 4 | 5 | 5 |
| | ALC_CMS | 1 | 2 | 3 | 4 | 5 | 5 | 5 |
| | ALC_DEL | | 1 | 1 | 1 | 1 | 1 | 1 |
| | ALC_DVS | | | 1 | 1 | 1 | 2 | 2 |
| | ALC_FLR | | | | | | | |
| | ALC_LCD | | | 1 | 1 | 1 | 1 | 2 |
| | ALC_TAT | | | | 1 | 2 | 3 | 3 |
| Security Target evaluation | ASE_CCL | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | ASE_ECD | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | ASE_INT | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | ASE_OBJ | 1 | 2 | 2 | 2 | 2 | 2 | 2 |
| | ASE_REQ | 1 | 2 | 2 | 2 | 2 | 2 | 2 |
| | ASE_SPD | | 1 | 1 | 1 | 1 | 1 | 1 |
| | ASE_TSS | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Tests | ATE_COV | | 1 | 2 | 2 | 2 | 3 | 3 |
| | ATE_DPT | | | 1 | 2 | 3 | 3 | 4 |
| | ATE_FUN | | 1 | 1 | 1 | 1 | 2 | 2 |
| | ATE_IND | 1 | 2 | 2 | 2 | 2 | 2 | 3 |
| Vulnerability assessment | AVA_VAN | 1 | 2 | 2 | 3 | 4 | 5 | 5 |

# Analogy of key terms

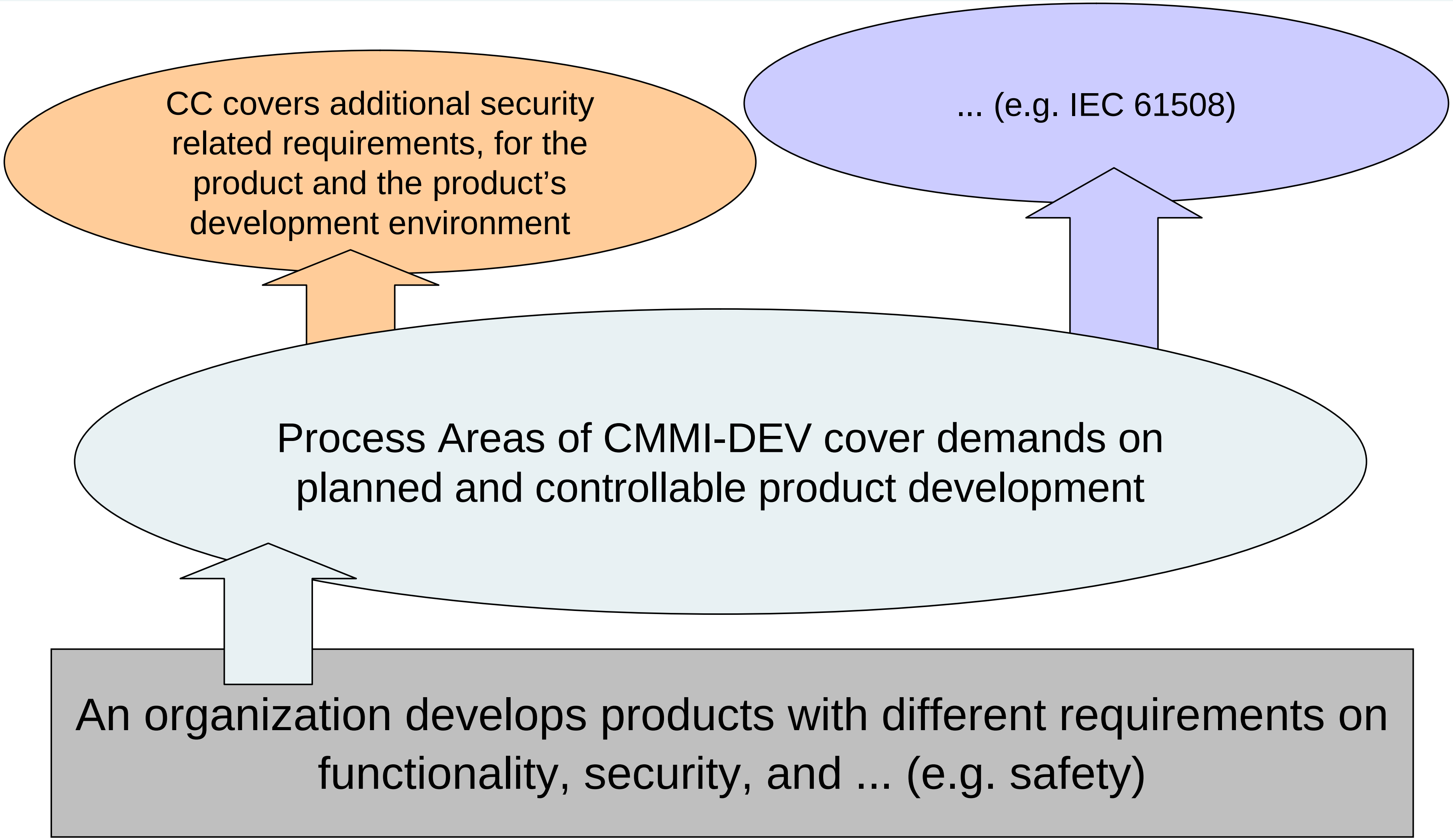
| | |
|---|---|
| **Process Area** | **Assurance Family** |
| **PA Category** | **Assurance Class** |
| **Capability Level** | **Assurance Component Leveling** |
| **Maturity Level** | **EAL** |
| **Addition** | **Extension** |

***Both, CMMI and CC, represent state of the art concepts and culmination of decades of experiences***

# Contents

1. Status Quo
2. CMMI® for Development
3. Striking Analogies
4. **Combining Standards**
5. Conclusion

# General idea



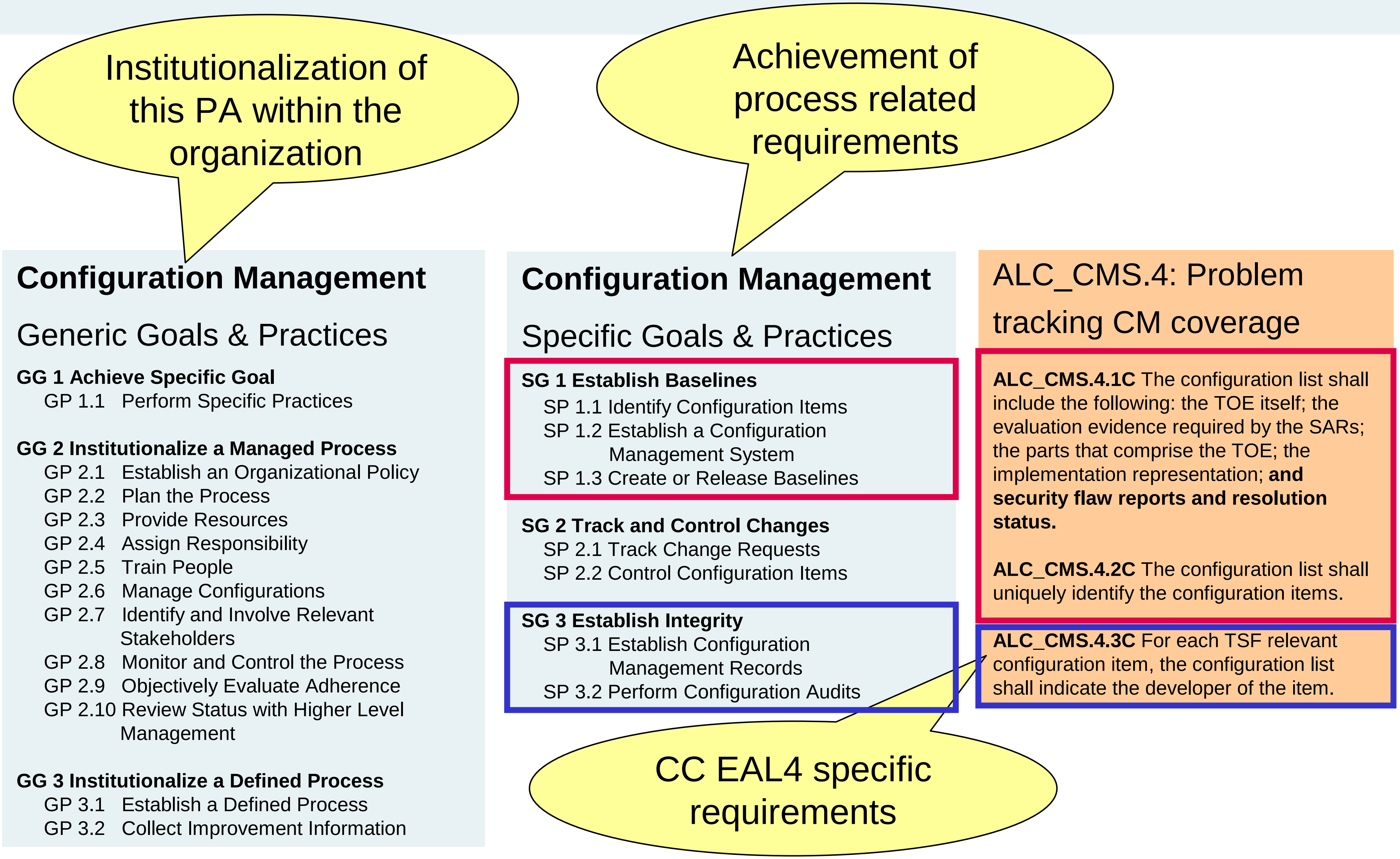
CC covers additional security related requirements, for the product and the product’s development environment

... (e.g. IEC 61508)

Process Areas of CMMI-DEV cover demands on planned and controllable product development

An organization develops products with different requirements on functionality, security, and ... (e.g. safety)

# Example: ALC_CMS (CM Scope)



Institutionalization of this PA within the organization

Achievement of process related requirements

**Configuration Management**

Generic Goals & Practices

**GG 1 Achieve Specific Goal**
GP 1.1 Perform Specific Practices

**GG 2 Institutionalize a Managed Process**
GP 2.1 Establish an Organizational Policy
GP 2.2 Plan the Process
GP 2.3 Provide Resources
GP 2.4 Assign Responsibility
GP 2.5 Train People
GP 2.6 Manage Configurations
GP 2.7 Identify and Involve Relevant Stakeholders
GP 2.8 Monitor and Control the Process
GP 2.9 Objectively Evaluate Adherence
GP 2.10 Review Status with Higher Level Management

**GG 3 Institutionalize a Defined Process**
GP 3.1 Establish a Defined Process
GP 3.2 Collect Improvement Information

**Configuration Management**

Specific Goals & Practices

**SG 1 Establish Baselines**
SP 1.1 Identify Configuration Items
SP 1.2 Establish a Configuration Management System
SP 1.3 Create or Release Baselines

**SG 2 Track and Control Changes**
SP 2.1 Track Change Requests
SP 2.2 Control Configuration Items

**SG 3 Establish Integrity**
SP 3.1 Establish Configuration Management Records
SP 3.2 Perform Configuration Audits

ALC_CMS.4: Problem tracking CM coverage

**ALC_CMS.4.1C** The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; **and security flaw reports and resolution status.**

**ALC_CMS.4.2C** The configuration list shall uniquely identify the configuration items.

**ALC_CMS.4.3C** For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

CC EAL4 specific requirements

# Activities and (first) results

Ø Focused on EAL4

Ø Bi-directional “mapping” and parts of the integration CC/CMMI-DEV done

Ø EAL4 does not require any addition of new CMMI-DEV process areas

Ø CMMI-DEV specific goal needs to be added ( à ALC_DVS)

Ø Lots of additions to specific practices in engineering, project management, and support will be needed

Ø Lots of additions to the CMMI-DEV informative material necessary

# Contents

1. Status Quo
2. CMMI® for Development
3. Striking Analogies
4. Combining Standards
5. **Conclusion**

# Conclusion and next steps

Ø Experience shows that efficiently developing high quality/security products requires managing the engineering processes

Ø In this respect CC needs to evolve or be combined with engineering standards

Ø Combining CMMI-DEV and CC is feasible

  Ø e.g. EAL4 would require Capability Level 3 of quite a few CMMI Process Areas

Ø Piloting with customers will follow

Ø Models will be implemented in a web based tool, supporting

  Ø reference models

  Ø process definition

  Ø management

Gracias 谢谢您

# Thank you!

Grazie

Danke

Merci

謝謝您

Takk

Obrigado Bedankt

# TÜV INFORMATIONSTECHNIK GMBH
## Member of TÜV NORD Group

Wolfgang Peter
Director Evaluation Body for IT Security

Langemarckstr. 20
D-45141 Essen

Phone: +49 201 8999 – 624
Fax: +49 201 8999 – 666
E-Mail: w.peter@tuvit.de
URL: www.tuvit.net